INFORMATION Management Conference

PKI Panel

Transformation through Partnerships

Future of PKI for DOE

Lynn Kluegel

April 17, 2012

Los Alamos NATIONAL LABORATORY EST. 1943

Unclassified

Operated by Los Alamos National Security, LLC for the U.S. Department of Energy's NNSA

LA-UR-12-20522

INFORMATION Management Conference

Immediate Benefits of the SSP

- Cost Savings for user certificates
- Key history maintained
- Expert help with issues
  - Improved service delivery
- Connectivity to Federal Bridge / Common Policy trusted sites
  - Compliance with Federal Policy
  - Increased span of secure communications to Federal community and business partners

Long Term Benefits of the SSP

- Easier integration with HSPD-12 PIV badges
  - Federal and DOE ICAM roadmaps depend on a robust, trusted PKI foundation
- Timely update of software versions to match current OS and email version
- Compliance with Federal Policy
  - SSP is responsible for maintaining trust

INFORMATION Management Conference

Current DOE PKI Sites

- RA Sites
  - Sites currently hosted by HQ CA
  - Once users are moved to SSP, operations will be similar if not the same for RA sites
  - SSP will need to ensure that RA procedures are being followed
    - May be refresher training
    - Regular audits will keep accreditation
- CA Sites
  - Sites running a Certificate Authority (CA) that is trusted by the current DOE PKI framework
  - LLNL, LANL,PNNL, ORNL, Sandia, Pantex, Y-12, KCP, HQ

INFORMATION Management Conference

PKI Certificates

- Deployment of PKI Certificates
  - Individual user certificates
    - Encryption of email and data files
    - Digital Signature of email and data files
  - Individual user certificates (at some sites) are also used for:
    - Digital Signature in Document Workflow applications or systems
    - Digital Signature for Business Processes (such as Time and Effort systems)

PKI Certificates (continued)

- Deployment of PKI Certificates
  - Locally generated SSL certificates are employed at some sites for:
    - Huge cost savings ($2. Versus $200.)
    - Internal web sites and internal server applications
    - Commercial SSL certificates are still needed when dealing with external customers
  - Some sites employ locally generated machine/device certificates for:
    - Verifying machine membership on the network
    - Wireless access

Note: In the future these certificates must comply with DOE and Federal Policy guidelines.

PKI Certificates (continued-2)

- Deployment of PKI Certificates
  - Windows Domain Controller certificates
    - PIV badge and Smart Card logins
  - Some sites have developed customized locally built ICAM-like systems that:
    - Automate processes triggered by HR events
    - Provision/de-provision accounts based on HR data
    - Manage user resources and approvals
    - These locally developed systems should be able to transition nicely to commercial ICAM solutions

Future of PKI for DOE

- DOE PKI Technical Working Group (TWG)
  - Moving some of the common certificates such as user certificates to be managed by an SSP will hopefully allow sites to work on new products and systems that require or employ certificates
  - Collaboration is the best way to accomplish what we all need.
    - Mobile Device Focus Group
      - Researched and provided data for risk assessment of Good Application installed on iOS devices
      - Resolved issues with SMIME in the Good Applications
    - Entrust Client Focus Group

Questions?

Membership and information on the DOE PKI TWG

Send email to dlk@lanl.gov